## REMARKS

The present Amendment cancels claims 1-22 and adds new claims 23-44. Therefore, the present application has pending claims 23-44.

The Examiner indicated that the references in the specification were not in a proper Information Disclosure Statement to satisfy the requirement of 37 CFR §1.98(b). Attached herewith is a PTO-1449 providing a listing of said references. An indication that the Information Disclosure Statement has been considered is respectfully requested.

Claims 1, 2, 6 and 18 stand objected to due to informalities noted by the Examiner. As indicated above, claims 1, 2, 6 and 18 were canceled. Therefore, this objection is rendered moot.

Claims 14 and 18 stand rejected under 35 USC §112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regards as their invention. As indicated above, claims 14 and 18 were canceled. Therefore, this rejection is rendered moot. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

Claims 1-22 stand rejected under 35 USC §103(a) as being unpatentable over Cramer (U.S. Patent No. 6,697,488). As indicated above, claims 1-22 were canceled. Therefore, this rejection is rendered moot. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

The features of the present invention as recited in new claims 23-44 are not anticipated nor rendered obvious by Cramer. Cramer is directed to a scheme with improve the security of encrypted data or information by using a practical public

cryptosystem that is able to resist adaptive attacks. According to Cramer, the scheme does not leak any information of the secret of the used key by generating an extended private key and public key. As per Cramer, a message m, also referred to as plaintext, can be encrypted to obtain a cipher text t by using the public key. This cipher text t can be transmitted over an insecure channel such as the internet so that only a recipient with the right private key is able to decrypt the cipher text t.

The proof of security according to the system taught by Cramer is based on standard assumptions which are the hardness of the Diffie-Hellman decision problem (DDH problem), wherein the DDH problem is very hard to solve due to the large calculation volume; and the collision intractability of the hash function, which is equivalent to the existence of universal one-way functions.

Cramer employs a hash function in the encryption algorithm as described in col. 7, line 50 to col. 8, line 21 and col. 11, line 60 to col. 12, line 34 thereof. Cramer also discloses a particular encryption method using a hash function and the hash value in claims 11 and 12 thereof.

The proof of security of the present invention as described, for example, on page 4, line 26 through page 7, line 4 of the present application relates to a security system which is also based on an assumption of the hardness of the Diffie-Hellman decision problem. However, the proof security of the present invention is not based on the above described assumption regarding the collision intractability of the hash function through which the existence of the universal one-way functions are provided. In the present invention, a hash function and a hash value are not used in the encryption process.

As is well known, various cryptographic schemes are based on various assumptions. However, such assumptions are not always realistic. The collision intractability of the hash function has not yet been verified. See page 3, line 27 to page 4, line 24 of the present application. Therefore, contrary to Cramer, the present invention does not rely on the unverified assumption of the collision intractability of the hash function for encryption and as such is directed to an encryption process entirely different from Cramer.

Thus, as is quite clear from the above, the present invention is quite different from Cramer, particularly with regard to the assumptions upon. According to the present invention, hash functions and values are not used in the encryption process thereof. Therefore, the features of the present invention as recited in the claims are not taught or suggested by Cramer whether taken individually or in combination with any of the other references of record.

The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the references utilized in the rejection of claims 1-22.

In view of the foregoing amendments and remarks, applicants submit that claims 23-44 are in condition for allowance. Accordingly, early allowance of claims 23-44 is respectfully requested.

To the extent necessary, the applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417 (500.41092X00).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 684-1120

**FORM PTO-1449** U.S. Department of Commerce Patent and Trademark Office

**INFORMATION DISCLOSURE STATEMENT BY APPLICANT**

(Use several sheets if necessary)

| ATTY. DOCKET NO. | SERIAL NO. |
|---|---|
| 500.41092X00 | 10/046,224 |
| APPLICANT: M. NISHIOKA, et al | |
| FILING DATE: January 16, 2002 | GROUP: 2136 |

## U.S. PATENT DOCUMENTS

| EXAMINER INITIAL | | DOCUMENT NUMBER | DATE | NAME | CLASS | SUBCLASS | FILING DATE IF APPROPRIATE |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |



## FOREIGN PATENT DOCUMENTS

| | | DOCUMENT NUMBER | DATE | COUNTRY | CLASS | SUBCLASS | ABSTRACT YES | ABSTRACT NO |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

| | | |
|---|---|---|
| | | R. L. Rivest, et al "A method for obtaining digital signatures and public-key cryptosystems, Commun. of the ACM, vol. 21, No. 2. pp. 120-126, 1978. |
| | | V. S. Miller, Use of elliptic curves in Cryptography, Proc. of Crypto '85, LNCS218, Springer-Verlag, pp. 417-426, 1985. |
| | | N. Koblitz, Elliptic Curve Crytosystems, Math. Comp. 48, 177, pp. 203-209, 1987. |

| EXAMINER | DATE CONSIDERED |
|---|---|
| | |

**EXAMINER:** Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

| FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office | ATTY. DOCKET NO. | SERIAL NO. |
|---|---|---|
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT | 500.41092X00 | 10/046,224 |
| (Use several sheets if necessary) | APPLICANT: M. NISHIOKA, et al | |
| | FILING DATE: January 16, 2002 | GROUP: 2136 |

## U.S. PATENT DOCUMENTS

| EXAMINER INITIAL | | DOCUMENT NUMBER | DATE | NAME | CLASS | SUBCLASS | FILING DATE IF APPROPRIATE |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |



## FOREIGN PATENT DOCUMENTS

| | | DOCUMENT NUMBER | DATE | COUNTRY | CLASS | SUBCLASS | ABSTRACT YES | ABSTRACT NO |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

| | | |
|---|---|---|
| | | M. O. Rabin, Digital Signatures and Public-key Encryptions as Intractable as Factorization, MIT, Technical Report, MIT/LCSTRANSMISSION-212, 1979. |
| | | T. El Gamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE, Trans. on Information Theory, IT-31, 4, pp. 469-472, 1985. |
| | | S. Goldwasser, et al Probabilistic Encryption, JCSS, 28, 2, pp. 270-299, 1984. |

| EXAMINER | DATE CONSIDERED |
|---|---|
| | |

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

| FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office | ATTY. DOCKET NO. | SERIAL NO. |
|---|---|---|
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT | 500.41092X00 | 10/046,224 |
| (Use several sheets if necessary) | APPLICANT: M. NISHIOKA, et al | |
| | FILING DATE: January 16, 2002 | GROUP: 2136 |

## U.S. PATENT DOCUMENTS

| EXAMINER INITIAL | | DOCUMENT NUMBER | DATE | NAME | CLASS | SUBCLASS | FILING DATE IF APPROPRIATE |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |



## FOREIGN PATENT DOCUMENTS

| | | DOCUMENT NUMBER | DATE | COUNTRY | CLASS | SUBCLASS | ABSTRACT YES | ABSTRACT NO |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

| | | |
|---|---|---|
| | | M. Blum et al, An Efficient Probabilistic Public-key Encryption Scheme which hides all Partial Information, Proc. of Crypto '84, LNCS196, Springer-Verlag, pp. 289-299, 1985. |
| | | S. Goldwasser, et al, Lecture Notes on Cryptography, http:/www-cse, ucsd.edu/users/mihir/1997. |
| | | T. Okamoto, et al, A new Public-key Cryptosystem as Secure as Factoring, Proc. of Eurocrypt '98, LNCS1403, Springer Veriag, pp. 308-318, 1998. |

| EXAMINER | DATE CONSIDERED |
|---|---|

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

| FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office | ATTY. DOCKET NO. | SERIAL NO. |
|---|---|---|
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT | 500.41092X00 | 10/046,224 |
| (Use several sheets if necessary) | APPLICANT: M. NISHIOKA, et al | |
| | FILING DATE: January 16, 2002 | GROUP: 2136 |

## U.S. PATENT DOCUMENTS

| EXAMINER INITIAL | | DOCUMENT NUMBER | DATE | NAME | CLASS | SUBCLASS | FILING DATE IF APPROPRIATE |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |



## FOREIGN PATENT DOCUMENTS

| | | DOCUMENT NUMBER | DATE | COUNTRY | CLASS | SUBCLASS | ABSTRACT YES | ABSTRACT NO |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

| | | |
|---|---|---|
| | | D. Dolve, et al Non-Malleable Cryptography, In 23rd Annual ACM Symposium on Theory of Computing, pp. 542-552, 1991. |
| | | M. Naor, et al Public-key Cryptosystems Provably Secure Against Chosen Ciphertext Attacks, Proc. of STOC, ACM Press, pp. 427-437, 1990. |
| | | M. Bellare, et al "Optimal Asymmetric Encryption How to Encrypt with RSA, Proc. of Eurocrypt '94, LNCS950, Springer Verlag, pp. 92-111, 1994. |

| EXAMINER | DATE CONSIDERED |
|---|---|

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

| FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office | ATTY. DOCKET NO. 500.41092X00 | SERIAL NO. 10/046,224 |
|---|---|---|
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use several sheets if necessary) | APPLICANT M. NISHIOKA, et al | |
| | FILING DATE January 16, 2002 | GROUP 2136 |

## U.S. PATENT DOCUMENTS

| EXAMINER INITIAL | | DOCUMENT NUMBER | DATE | NAME | CLASS | SUBCLASS | FILING DATE IF APPROPRIATE |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |



## FOREIGN PATENT DOCUMENTS

| | | DOCUMENT NUMBER | DATE | COUNTRY | CLASS | SUBCLASS | ABSTRACT YES | ABSTRACT NO |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

| | | |
|---|---|---|
| | | R. Cramer et al, A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack, Proc. of Crypto '98, LNCS1462, Springer-Verlag, pp. 13-25, 1998. |
| | | M. Bellare, et al Relations Among Notions of Security for Public-key Encryption Schemes, Proc. of Crypto '98, LNCS1462, Springer Verlag, pp. 26-45, 1998. |
| | | |

| EXAMINER | DATE CONSIDERED |
|---|---|

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.